

FIG. 1

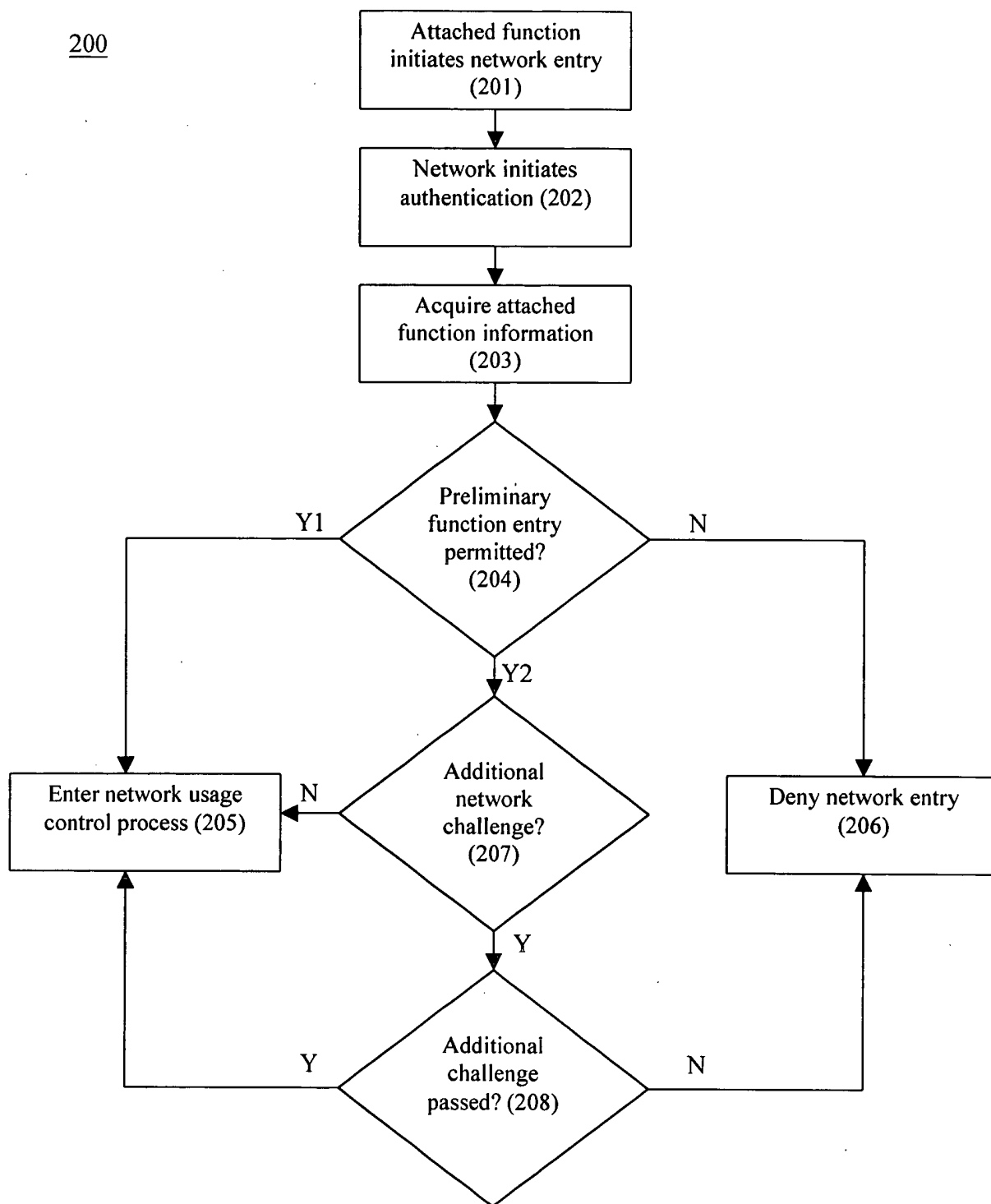


FIG. 2

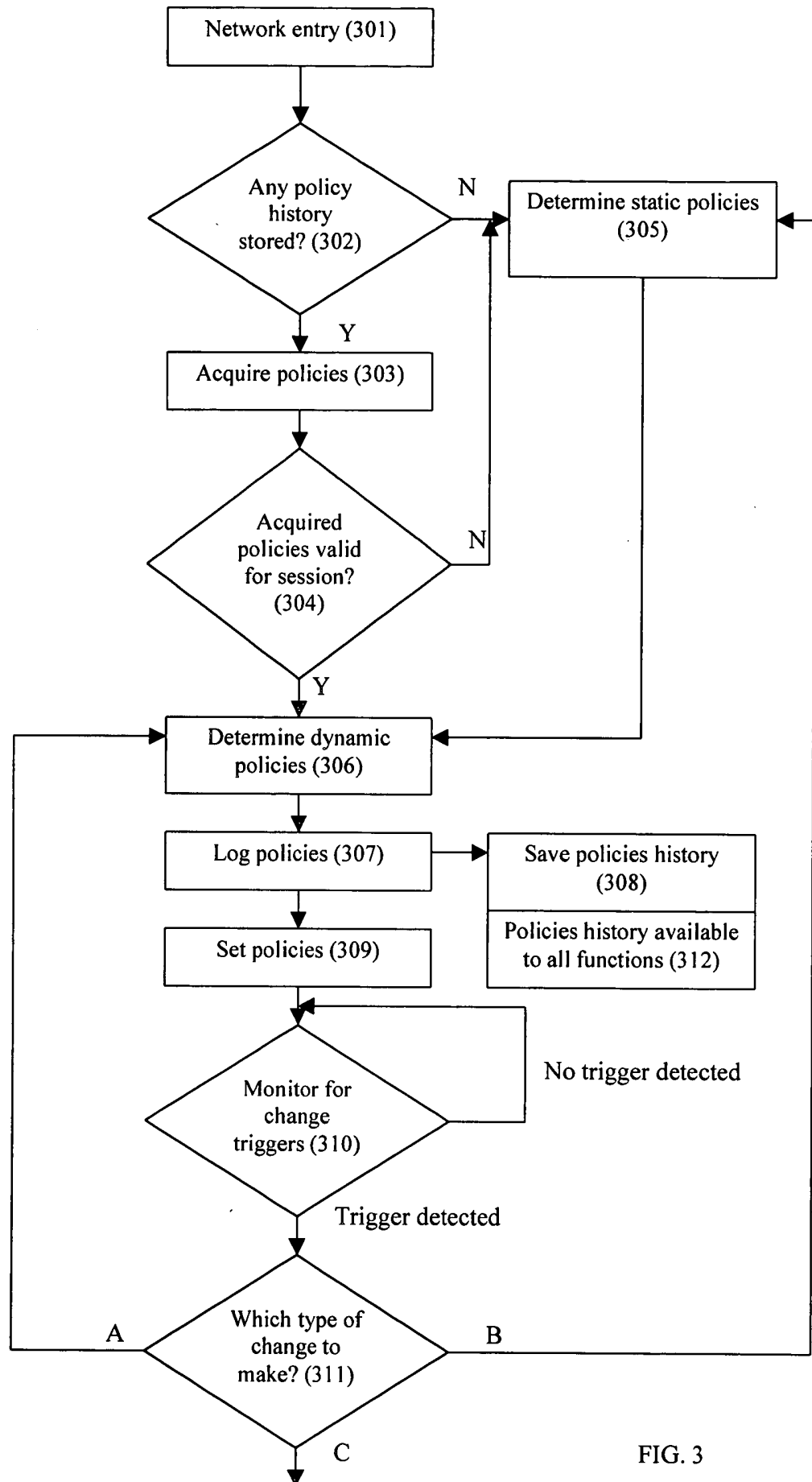


FIG. 3

<u>Information</u>	<u>Change triggers</u>	<u>Policies</u>
User ID	Time Outs	Internet Access Only
Device type	Link Changes, up/down, speed	IEEE 802.1X Authentication Required
Device Location	User Changes	Disable Unused Ports
Access Device	Device Changes	Reset On Intrusion Detection
Access Location	Device Additions	Specific Application Access Only
Port Type and Speed	Network Service Changes	Priority Access
Users Per Port	Access Device Changes	Application Bandwidth Limits
Devices Per Port	Location Changes	Port Based Priority
Devices Per User	IDS or Firewall Events	L2 Protocol Filter/Access List
Time Of Access	Application Access Request	Multi-step authentication
Application Used	Priority Change Request	Wireless/Wired Access Rules
Application Priority	Protocol Change	Log All Traffic
Port Security	Additional Wireless User	Set Group Characteristic Rules
Requested Priority	Administrator Set Policy Changes	New Session Logging
Ethernet Protocol	Bandwidth Changes	Flow Logging
Level of Trust	Routing Link Cost Changes	Limit Port Setting (speed, priority, ACL)
Virus Scan level	RMON or Other Monitored Events	Phone Access Only
Operating System Type and Version	Dynamic Policy Changes (local)	Time-of-Day Based Access (any policy)
Network system	Dynamic Policy Changes (remote)	Stateful Inspection
	Network system changes	

FIG. 4